

AMENDMENTS TO THE CLAIMS

1-2. (Cancelled)

3. (Currently amended) ~~A~~ The group management device of Claim 69, wherein that  
~~manages a group, comprising:~~  
~~a reception unit operable to receive from a member device, a request for~~  
~~registration to the group;~~  
~~a judging unit operable, upon receiving the request, if the member device is~~  
~~authenticated as being a the legitimate device, the judging unit judges to judge whether a~~  
~~the registered number of member devices is less than a maximum number of member~~  
~~devices registerable in the group, and to register the member device~~  
~~when judged in the affirmative, the judging unit registers the member device,; and~~  
~~— a communication unit operable, when the judging unit judges in the~~  
~~affirmative, to output to the member device, common secret information unique to the~~  
~~group.~~

4. (Currently amended) The group management device of claim 3, wherein  
the judging unit includes:  
an authentication subunit operable to hold a second initial value, and to  
authenticate the member device, using the second initial value and a first initial value  
held by the member device; and  
a device-number judging subunit operable, when authentication is successful, to  
judge whether the registered number is less than the maximum number,  
the common secret information outputted by the communication unit shows  
“registered in the group”, and  
the member device receives and holds the outputted common secret information,  
and deactivates the first initial value.

5. (Original) The group management device of claim 4, wherein  
the first and second initial values show “unregistered in the group”.

6. (Original) The group management device of claim 4, wherein  
the first and second initial values show "unregistered in any group".
7. (Original) The group management device of claim 3, further comprising:  
a generating unit operable to generate the common secret information, wherein  
the communication unit outputs the generated common secret information to the  
member device.
8. (Original) The group management device of claim 3, wherein  
the common secret information is generated by a management device outside of  
the group,  
the judging unit receives the common secret information from the out-group  
management device, and  
the communication unit outputs the received common secret information to the  
member device.
9. (Currently amended) The group management device of claim 3, wherein  
the reception unit, on receipt of the registration request, notifies the receipt to a  
management device outside of the group,  
the out-group management device judges whether the registered number is less  
than the maximum number,  
the judging unit, instead of judging whether the registered number is less than the  
maximum number, receives a judgment result from the out-group management device,  
and  
the communication unit outputs the common secret information to the member  
device, when the judgment result shows that the registered number is less than the  
maximum number.
10. (Original) The group management device of claim 3, wherein  
the maximum number is formed from a first maximum number and a second  
maximum number, and

the judging unit judges whether the registered number is less than one of the first maximum number and the second maximum number, and registers the member device when judged in the affirmative.

11. (Original) The group management device of claim 10, wherein

the first maximum number is the number of member devices, out of the maximum number, connectable to the group management device, and the second maximum number is the number of member devices, out of the maximum number, not connectable to the group management device, and

the judging unit judges, (i) when the member device is connectable to the group management device, whether the registered number of connectable member devices is less than the first maximum number, and (ii) when the member device is not connectable to the group management device, whether the registered number of non-connectable member devices is less than the second maximum number.

12. (Currently amended) The group management device of claim 3, wherein

the communication unit outputs to another group management device, a request inquiring whether the member device is registerable in the other group management device,

the other group management device receives the inquiry request, judges whether a registered number of member devices is less than a maximum number of member devices registerable with the other group management device, and when judged in the affirmative, registers the member device and outputs the common secret information to the group management device, and

the communication unit, on receipt of the common secret information from the other group management device, outputs the received common secret information to the member device.

13. (Original) The group management device of claim 3, wherein

the judging unit functions to resist invalid access from outside, and

the maximum number and the common secret information are stored in an area that is unreadable/unwritable from outside.

14. (Original) The group management device of claim 13, wherein the judging unit is included in a portable module that is mountable in the group management device.
15. (Original) The group management device of claim 3, wherein the judging unit stores a remaining number obtained by subtracting the registered number from the maximum number, and on receipt by the reception unit of the registration request, judges whether the remaining number is "0", and when judged that the remaining number is not "0", the communication unit outputs the common secret information to the member device and the judging unit subtracts "1" from the remaining number.
16. (Currently amended) The group management device of claim 3, wherein the reception unit, after the outputting of the common secret information, receives from the member device, a request for withdrawal from the group, the communication unit, on receipt by the reception unit of the withdrawal request, outputs to the member device, a notification indicating to delete the common secret information, the reception unit receives from the member device, a notification showing that deletion of the common secret information has been completed, and the judging unit, on receipt by the reception unit of the deletion-completed notification, reduces the registered number.
17. (Cancelled)
18. (Original) The group management device of claim 3, wherein the judging unit receives from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in

accordance with the received number, and sets the received number as the maximum number.

19. (Currently amended) The group management device of claim 3, wherein the judging unit newly acquires from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the acquired number, and adds the acquired number to the maximum number to obtain a new maximum number.

20. (Original) The group management device of claim 3, wherein the reception unit, after the outputting of the common secret information, receives a communication request from the member device, the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and the communication unit communicates with the member device when authentication is successful.

21. (Original) The group management device of claim 3, further comprising: a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; and an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key, wherein the communication unit outputs the encrypted content and the encrypted content key to the member device.

22. (Original) The group management device of claim 21, wherein the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and shares a session key with the member device, using the common secret information, and the encryption unit, when authentication is successful, encrypts the content key using the shared session key.

23. (Original) The group management device of claim 3, wherein the communication unit stores therein the common secret information, newly receives a different piece of common secret information, overwrites the stored common secret information with the newly received common secret information, and outputs, regularly or irregularly, the newly received common secret information to the member device.

24. (Original) The group management device of claim 3, further comprising:  
a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key;  
an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key; and  
a writing unit operable to write the encrypted content and the encrypted content key to a portable recordable medium.

25. (Original) The group management device of claim 24, wherein the received registration request includes an identifier identifying the member device, and  
the encryption unit encrypts the content key using a key generated based on the common secret information and the identifier, to generate the encrypted content key.

26. (Original) The group management device of claim 24,  
the encryption unit encrypts the content key using a key generated based on the common secret information and an identifier unique to the portable recordable medium.

27. (Original) The group management device of claim 3, further including:  
a holding unit operable to hold, in correspondence with identifiers that each identify a different group, (i) common secret information unique to the group and (ii) a maximum number of member devices registerable in the group, wherein  
the received registration request includes one of the identifiers,

the judging unit, on receipt by the reception unit of the registration request, judges whether the number of member devices registered in a group identified by the identifier is less than a maximum number corresponding to the identifier, and when judged in the affirmative, registers the member device in the group and selects common secret information corresponding to the identifier, and

the communication unit outputs the selected common secret information to the member device.

28. (Original) The group management device of claim 3, wherein the received registration request requests the registration of a predetermined number of other member devices,

the judging unit judges whether an aggregate number obtained by adding the predetermined number to the registered number is less than the maximum number, and when judged in the affirmative, generates a permission right permitting a copying of the common secret information to the predetermined number of member devices, and the permission right is attached to the outputted common secret information.

29. (Original) The group management device of claim 3, wherein the received registration request includes a first identifier unique to the member device,

the judging unit stores therein the first identifier,

the reception unit, after the outputting of the common secret information, receives a second identifier unique to the member device,

the judging unit judges whether the second identifier matches the first identifier, and

the communication unit, when judged that the first and second identifiers match, again outputs the common secret information to the member device.

30. (Original) The group management device of claim 3, wherein when the group management device is determined to be a new group management device for managing a new group formed by combining groups managed by a plurality of

group management devices, the communication unit outputs to member devices registered in the groups, new common secret information unique to the new group, and

when one of the other group management devices is determined to be the new group management device, the group management device further comprises:

a receiving unit operable to receive the new common secret information from the other group management device; and

a holding unit operable to hold the received new common secret information.

31. (Currently amended) The group management device of claim 30, wherein the communication unit determines, in conjunction with the other group management devices, one of the group management devices to be the new group management device.

32. (Original) The group management device of claim 31, wherein the holding unit stores therein a priority level of the group management device, and the communication unit determines, out of the stored priority level and priority levels of the other group management devices, the group management device having the highest priority level to be the new group management device.

33. (Original) The group management device of claim 30, wherein each member device registered in the groups managed by the group management device and the other group management devices has a priority level, and when the group management device is determined to be the new group management device, the reception unit acquires the priority levels of the member devices, the group management device further comprises a selecting unit operable to select, in order from highest to lowest of the acquired priority levels, member devices for registration in the new group, the selected number of member devices being less than or equal to a maximum number of member devices registerable in the new group, and the communication unit outputs the new common secret information to the selected member devices.



34. (Original) The group management device of claim 3, further comprising:  
a determining unit operable, after the outputting of the common secret information, to determine a member device registered in the group to be another group management device; and  
a dividing unit operable to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device, and  
the communication unit outputs, after the dividing by the dividing unit, a different piece of common secret information to the member devices to be registered in the group managed by the group management device.

35-48. (Cancelled)

49. (Currently amended) The A member device that uses a content after registering in a group managed by a group managing device, comprising: of claim 35, wherein  
a requesting unit operable to request the group management device for registration in the group;  
a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, the received common secret information unique to the group that includes information showing a valid period information showing a valid period during which of use of the common secret information is permitted in the member device; and  
the a holding unit operable to hold the received common secret information, to monitors an elapse of the valid period, and to deletes the common secret information when the valid period ends.

50-68. (Cancelled)

69. (New) A group management device that manages a group, comprising:

a reception unit operable to receive, from a member device, a request for registration in the group;

a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group,

(ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and

(iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends; and

a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information and the valid period information.

70. (New) A group formation/management system comprising:

a group management device; and

a group member device,

the group management device including:

a reception unit operable to receive, from a member device, a request for registration in the group;

a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group,

(ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and

(iii) to monitor an elapse of the valid period, and reduce the registered number when the valid period ends; and

a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information and the valid period information, and

the group member device including:

a requesting unit operable to request the group management device for registration in the group;

a receiving unit operable to be authenticated by the group management device, and to receive, from the group management device, the common secret information and the valid period information; and

a holding unit operable to hold the received common secret information, to monitor the elapse of the valid period, and to delete the common secret information when the valid period ends.

71. (New) A group management method used in a group management device that manages a group, the group management method comprising:

receiving, from a member device, a request for registration in the group;

(i) upon receiving the request, if the member device is authenticated as being a legitimate device, judging whether a registered number of member devices is less than a maximum number of member devices registerable in the group,

(ii) when judged in the affirmative, issuing valid period information showing a valid period of use of common secret information unique to the group for the member device, and increasing the registered number, and

(iii) monitoring an elapse of the valid period and reducing the registered number when the valid period ends; and

when judged in the affirmative, outputting to the member device the common secret information and the valid period information.

72. (New) A recording medium storing a computer program used in a group management device that manages a group, the computer program comprising:

receiving, from a member device, a request for registration in the group;

(i) upon receiving the request, if the member device is authenticated as being a legitimate device, judging whether a registered number of member devices is less than a maximum number of member devices registerable in the group,

(ii) when judged in the affirmative, issuing valid period information showing a valid period of use of common secret information unique to the group for the member device, and increasing the registered number, and

(iii) monitoring an elapse of the valid period and reducing the registered number when the valid period ends; and

when judged in the affirmative, outputting to the member device, the common secret information and the valid period information.

73. (New) A control method used in a group management device that manages a group, the control method comprising:

requesting the group management device for registration in the group;

being authenticated by the group management device and receiving, from the group management device, common secret information unique to the group that includes valid period information showing a valid period of use of the common secret information; and

holding the received common secret information, monitoring an elapse of the valid period, and deleting the common secret information when the valid period ends.

74. (New) A recording medium storing a computer program used in a group management device that manages a group, the computer program comprising:

requesting the group management device for registration in the group;

being authenticated by the group management device and receiving, from the group management device, common secret information unique to the group that includes valid period information showing a valid period of use of the common secret information; and

holding the received common secret information, monitoring an elapse of the valid period and deleting the common secret information when the valid period ends.